Emerging Standards

Editors: Ramaswamy Chandramouli, mouli@nist.gov
Tim Grance, tim.grance@nist.gov
Rick Kuhn, kuhn@nist.gov
Susan Landau, susan.landau@sun.com

Toward Secure Routing Infrastructures

Routing infrastructures—the protocols, data, and algorithms that compute paths through interconnected network devices—are possibly the most vital, complex, and fragile components in the global information infrastructure. They are also the least protected.

Doug Montgomery
US National Institute of Standards and Technology

Sandra Murphy
Sparta

Routing systems underlie nearly all data communications and are found at multiple layers of the network architecture. From layer-2 systems used to interconnect LAN switches to the multiple layer-3 systems used for Internet Protocol (IP) routing to content- and context-based systems at layer 4 and above, routing systems provide the fundamental service of organizing sets of interconnected network devices into viable end-to-end data paths.

Today, the IP routing infrastructure is the area of greatest security concern. As the glue that interconnects public and private networks, IP routing infrastructures are some of the largest, most complex control systems in the modern information infrastructure. In the public Internet, for example, the IP routing infrastructure comprises tens of thousands of individual routing domains, each employing numerous distinct protocols and technologies that operate as a loosely hierarchical but interdependent global distributed system. In this article, we look at the current state of, and practical prospects for, security in IP routing infrastructures.

Internet routing system vulnerabilities

The design objectives and technologies underlying IP routing protocols vary greatly, according to their applications. The most common and important scope is the one focused on unicast routing among fixed (that is, nonmobile) hosts. The routing system for this environment consists of a two-level hierarchy of protocols:

- *Intradomain* protocols (or interior gateway protocols [IGPs]) are designed for use within single administrative or management domains (called autonomous systems [ASs]) with sparse connectivity and little control of topologies. IGPs typically optimize exploiting all possible paths to achieve robustness and responsiveness with little or no concern for issues of policy and trust. Examples of IGPs deployed in the Internet today include Open Shortest Path First (OSPF), Intermediate System to Intermediate System (IS-IS), and proprietary protocols such as Cisco's Enhanced Interior Gateway Routing Protocol (EIGRP).
- *Interdomain* protocols (or exterior gateway protocols [EGPs]) are designed to route between ASs—an environment in which administrators have greater control of the local topology but little if any trust exists between remote domains. EGPs typically optimize policy enforcement (that is, using only policy-feasible paths) and global stability over responsiveness and ultimate connectivity. The only significant EGP currently deployed in the Internet is the Border Gateway Protocol (BGP).

Most large-scale routing systems are somewhat vulnerable, given that their control algorithms are carefully tuned to address the inherent tradeoffs between responsiveness and stability based on typical nonmalicious failure scenarios. That is, they aren't typically designed to address focused, malicious attacks. This is particularly true in the BGP routing infrastructure. Although few documented attacks have focused on the routing infrastructures to date, we can't expect such luck to continue. As responses to common attacks continue to harden hosts and applications, those seeking to disrupt networks will shift their efforts to the underlying control systems. In fact, attacking routing systems is often an easier way to disable specific end applications or hosts.[1] The many threats to routing systems include distinct classes of insider and outsider attacks as well as nonmalicious failures and misconfigurations, all of which can potentially cause catastrophic network failures.[2] Thus far, for example, the most serious threats to the BGP infrastructure have come from misconfigurations that have led to widespread, long-standing network outages.[3] In fact, the most general formulation of the routing robustness problem addresses routing in the face Byzantine failures, in which some nodes operate in completely random ways.[4]

That said, the threats from malicious attack are both real and serious. All routing protocols currently deployed on the Internet are vulnerable to several classes of attack. The simplest, and perhaps most threatening, is the compromise and control of valid routers. Some reports suggest that would-be attackers can gain access to hundreds of BGP-speaking routers on the black market for a single stolen credit-card number. Even without compromised routers, the routing protocols and associated resources on routers are vulnerable to attack from remote nodes. Such attacks can focus on control-plane resources (for example, distributed denial-of-service attacks on routing protocols), the peering relationships among connected routers, or the data content of the protocol exchanges between peer routers. Attacks can also focus on lower-layer resources (such as physical links and protocols) that interconnect individual routers. In some cases, malicious parties can exploit, as attack vectors, the very mechanisms designed to enhance stability during typical failures.[5]

Among the many possible consequences of attacks on routing is the complete disabling or theft of data and control traffic for vast segments of global networks. Consequences include loss of connectivity (black holes and partitions, for example), eavesdropping (routing traffic through malicious nodes), suboptimal routing (using congested, delayed, or unstable paths), and routing system disruption (causing churn and instability in the routing protocols themselves, for instance). All currently deployed routing protocols are vulnerable to many, if not all, of these threat scenarios, and the risks will only increase as we expect more of routing systems through enhanced services such as traffic engineering and quality-of-service (QoS)-sensitive routing.

Practical challenges to secure routing

The usual risk–reward business issues that inhibit the adoption of many large-scale security technologies are partly responsible for the current situation with the routing infrastructure. To date neither the threat–consequence potentials nor the potential returns on investment have been apparent enough to encourage commercial entities to devote the necessary resources to develop and deploy more-secure infrastructures. The other, related, culprit is the absence of complete, viable, standardized security solutions for most routing technologies. Both the problem space (agreeing on the threats and security requirements) and the solution space (designing security extensions or new protocols) are extremely broad. (For further discussion, see the IETF Routing Protocol Security Requirements working group at www.ietf.org/html.charters/rpsec-charter.html.) In particular, routing protocols vary tremendously in their design and operation. No single security solution can address all routing protocols. Even within a single routing protocol different security techniques might be required to address peer-to-peer and multiparty communications, single-hop and multihop messages, and mutable and immutable data components.

Attempts to add cryptographic protections to routing protocols also run into challenges such as

- incomplete knowledge of network topology and difficulties with clock synchronization;
- multiple trust-relationship graphs (for example, address administration, intra- versus interdomain, and customer to service provider);
- routing services' need to bootstrap themselves, thus complicating techniques that depend on other components (such as public-key infrastructure systems, directories, and management systems) for basic startup operations.

Dynamic performance requirements also add some serious constraints on secure routing solutions. Many Internet routing systems typically face trade-offs between scalability and stability. The largest routing systems (such as global BGP) are distributed systems with poorly understood global convergence and stability properties. As a practical matter, added security mechanisms must not significantly change otherwise viable routing technologies' scalability or performance. Some practical requirements of operational routing systems include IGPs that offer subsecond convergence on very large enterprise networks; BGP's global operational scale of tens of thousands of domains and hundreds of thousands of networks; and mobile ad hoc networks' support for thousands of nodes constantly moving at vehicular speeds. Additional challenges include the performance constraints of the platforms on which routing protocols operate. At the core, for example, more than three orders of magnitude difference exist in the control and data planes' processing capabilities; at the mobile edge, battery life presents another important design constraint. Finally, we must address the practical problems of adoption and deployment, including a means for incremental or partial deployment, favorable benefit–risk models, and a viable means for day-to-day operations and management.

Routing security: Past, present, and future

Given the looming vulnerabilities and daunting problem space, what can we say about where we stand today and where to focus future efforts? No widely deployed secure routing protocols are in use today. The current state of the art in protecting our routing infrastructures relies on so-called best practices, which include various simplistic techniques (such as passwords, TCP

IETF routing security standards activities

The Internet Engineering Task Force (www.ietf.org) is the open standardization body for protocols used in the public Internet. The common security services specified for IETF standard routing protocols (Open Shortest Path First [OSPF], Intermediate System to Intermediate System [IS-IS], Border Gateway Protocol [BGP], and so on) are integrity and authentication between protocol neighbors. These protections are widely available in commercial implementations. Other routing protocols and networking services are layered over the common routing protocols—for virtual private networks (VPNs) and traffic engineering, for instance—and rely on the underlying protocols' security.

The protections in these standards are mainly keyed hashes based on the MD5 algorithm. Most of these designs have security issues—in some cases, the keyed hash computation is unsophisticated, whereas some other designs fail to provide for key rollover or migration to other algorithms. With long-standing concerns over MD5's security, IETF working groups have recently started efforts to move OSPF, IS-IS, and TCP MD5 to a better security footing. TCP MD5 is getting the most attention because it's used to protect the BGP interdomain routing protocol and therefore poses the widest risk. Different working groups have received at least three different proposals. Given that this issue combines TCP, routing, and security, the problem could require a cross-disciplinary group.

Not all routing protocol protections are cryptography-based. The Generalized TTL Security Mechanism (GTSM) defines a time-to-live (TTL)-based mechanism to help routers ensure that the packets they receive are from hosts one IP hop away. This helps to ensure that packets come from neighboring routers, without requiring cryptography. The last IETF meeting also saw the introduction of work that provides a threat analysis for network environments and recommends protection choices by environment. Well-received at presentations in several working group meetings, this work is likely to move forward.

The protections specified for IETF standard routing protocols focus on ensuring the integrity and authenticity of the connection

authentication, route filters, and private addressing) to mitigate the most rudimentary vulnerabilities and threats. The research and development community has been pursuing more complete solutions to the problem for the past 15 years, at both theoretical and practical levels, including developing specific extensions to commonly used protocols. In the late 1990s, several efforts proposed cryptographic extensions to BGP and OSPF. To date, however, few of these have achieved any significant level of commercial implementation or deployment. In several cases, the first-generation solutions failed to meet many of the performance and deployment constraints we mentioned because they optimized security concerns at all costs over those of scalability and performance.

Goverments and the standardization and development communities have recently shown renewed interest in routing security. (See, for example, the US Department of Homeland Security-sponsored Secure Protocols for the Routing Infrastructure [SPRI] project; www.cyber.st.dhs.gov/spri.html.) Within the Internet Engineering Task Force (IETF), working groups strive to understand existing routing protocols' threat and consequence models and to launch new efforts to better address the practical requirements and constraints of today's operational environments (see the "IETF routing security standards activities" sidebar). For example, some recent proposals for secure variants of BGP[6] aim to strike different balances between security and performance.

Looking to the future, we can identify several areas that require research and potentially fundamentally new approaches to routing systems and routing security, in order to provide better assurance than is practical today:

- *Secure protocol architectures*. New designs for the decomposition of routing and security functions should address the further decoupling of control and data planes and the incorporation of programmable technologies in the data plane.
- *Risk analysis*. New models must provide a better understanding of the potential risks associated with security vulnerabilities and other potential forms of focused, large-scale disruptions to routing systems.
- *Flexible and survivable secure routing*. Flexible designs that recognize security as just one vital component of the routing infrastructure's overall viability and survivability could address environments in which reputation management is a trust continuum, rather than a Boolean decision, thus letting systems selectively and dynamically adapt mechanisms to trade threat mitigations for performance, scalability, and cost concerns.
- *Secure routing systems*. System-level designs should explicitly integrate other security technologies such as intrusion- or anomaly-detection and firewalls as part of the secure routing system.
- *Efficient security mechanisms for routing*. New cryptographic techniques should ensure the authen-

between neighboring routers. More recently, the IETF has begun to energetically address the very different problem of preventing a faulty, misconfigured, or subverted router from causing widespread damage. The Routing Protocol Security Requirements (RPSec) and Secure Inter-Domain Routing (SIDR) working groups are now addressing the problems of routing security, with deliberate intent to consider these insider attacks.

The RPSec working group has recently completed work on a document entitled "Generic Threats to Routing Protocols," currently in the IETF RFC Editor queue.[1] Since then, the group has devoted energy to the "BGP Security Requirements" draft, which is nearing completion. It reached consensus on a requirement for authorization to originate a BGP route to a network, but no consensus exists on protecting more complex BGP-message attributes. The working group is now considering work on a BGP attack tree, OSPF vulnerabilities, and a summary of replay-related vulnerabilities in several different routing protocols.

The SIDR working group was chartered in 2006 to work on those requirements that achieve consensus in the RPSEC working group. The group is currently considering a public-key infrastructure (PKI) that would represent the authority to speak for an address, based on the current address-allocation hierarchy. Rooted PKIs have their critics among Internet service providers, so an important feature of this work is to allow the representation of different trust models. Work has barely begun on creating a specification for BGP route-origination authority, based on this PKI.

The state of security standards for multicast and mobile ad hoc routing protocols is much less well-established. Multicast routing protocols can presently rely only on the limited support for multicast addresses in the IP Security protocols. Mobile routing protocols present even more challenging security issues, due to their lack of infrastructure and trust models; the dynamic nature of neighbor relationships in mobile environments; and the presumed lack of resources on mobile nodes. Definitive security solutions for these areas are still essentially research problems.

Reference

1. A. Barbir, S. Murphy, and Y. Yang, "Generic Threats to Routing Protocols," IETF Internet draft, Oct. 2004; work in progress.

ticity, integrity, and freshness of routing information with better performance and fewer infrastructure requirements than those currently proposed.

- *Secure self-organizing networks*. Self-organizing networks (sensor, wireless ad hoc, large-scale peer-to-peer networks, and so on), especially those that can't assume the existence of a fixed infrastructure, pose significant security challenges, including secure group formation, membership management, and trust management between ephemeral groups.

We are entering a critical period in the evolution of routing infrastructures. The complexity of, and requirements imposed on, routing technologies continue to escalate. This capability–complexity growth spiral will increase the potential vulnerabilities to, and consequences of, focused routing system attacks. The current generation of standardization efforts is focused on adding a practical level of assurance to today's routing technologies. Future research directions point toward fundamentally new approaches to achieving tomorrow's secure routing infrastructures. □

Acknowledgments

Any mention of commercial products is for information only; it does not imply recommendation or endorsement by NIST.

References

1. L. Wang et al., "Protecting BGP Routes to Top Level DNS Servers," *Proc. 23rd Int'l Conf. Distributed Computing Systems* (ICDCS), IEEE CS Press, 2003, p. 322.
2. A. Barbir, S. Murphy, and Y. Yang, "Generic Threats to Routing Protocols," IETF Internet draft, Oct. 2004; work in progress.
3. R. Mahajan, D. Wetherall, and T. Anderson, "Understanding BGP Misconfiguration," *Proc. ACM SIGCOMM 2002*, ACM Press, 2002, pp. 3–16.
4. R. Perlman, *Network-Layer Protocols with Byzantine Robustness*, PhD thesis, Massachusetts Inst. of Tech., 1988; www.lcs.mit.edu/publications/pubs/pdf/MIT-LCS-TR-429.pdf.
5. K. Sriram et al., "Study of BGP Peering Session Attacks and Their Impacts on Routing Performance," to be published in *IEEE J. Selected Areas in Comm.*, special issue on network security, Oct. 2006.
6. K. Butler et al., *A Survey of BGP Security*, tech. report TD-5UGJ33, AT&T Labs–Research, Feb. 2004; www.patrickmcdaniel.org/pubs/td-5ugj33.pdf.

Doug Montgomery *is the manager of the Internetworking Technologies Research Group at the US National Institute of Standards and Technology. His research interests include Internet infrastructure protection, self-managing systems, network security, and network metrology. Montgomery has an MS in computer and information sciences from the University of Delaware. He is a member of the IEEE and IETF communities. Contact him at dougm@nist.gov.*

Sandra Murphy *is a principal computer scientist at Sparta. Her research interests include security in infrastructure protocols and distributed systems. Murphy has a PhD in computer science from the University of Maryland. She is a member of the IEEE and the ACM. She has served on program committees for the ISOC Network and Distributed Systems Security Symposium (NDSS), IEEE Conference on Open Architectures and Network Programming (OpenArch), and IFIP-TC6 International Working Conference on Active Networks. Contact her at sandra.murphy@sparta.com.*